AMENDMENTS TO THE CLAIMS

1. (Currently Amended) A processor comprising

memory; and

one or more execution units to load an authenticated code module into the memory, to lock the memory, to authenticate the ~~an~~ authenticated code module stored in the memory, and to execute the authenticated code module stored in the ~~private~~ memory in response to executing a launch instruction,

~~wherein components separate from the processor are prevented from altering the authenticated code module stored in the memory~~.

2. (Currently Amended) The processor of claim 1 further comprising a cache memory that provides the ~~private~~ memory.

3. (Canceled)

4. (Currently Amended) The processor of claim 2 ~~3~~ wherein the execution units lock the cache memory to prevent replacement of lines of the authenticated code module stored in the cache memory.

5. (Currently Amended) The processor of claim 1 wherein the execution units lock the ~~private~~ memory to prevent other processors from altering the authenticated code module stored in the ~~private~~ memory.

6. (Original) The processor of claim 1 further comprising a decoder to generate one or more opcodes for the launch instruction, wherein the execution units authenticate and execute the authenticated code module in response to executing the one or more opcodes.

7. (Original) The processor of claim 1 further comprising a key, wherein the execution units utilize the key to authenticate the authenticated code module.

8. (Previously Presented) The processor of claim 1, wherein the execution units retrieve a key specified by one or more operands of the launch instruction and use the key to authenticate the authenticated code module stored in the memory.

9. (Previously Presented) The processor of claim 1, wherein the execution units, in response to the launch instruction, retrieve a key from a chipset and use the key to authenticate the authenticated code module stored in the memory.

10. (Withdrawn) The processor of claim 1, wherein the execution units, in response to the launch instruction, retrieve a key from a token and use the key to authenticate the authenticated code module stored in the protected memory.

11. (Withdrawn) The processor of claim 1, wherein the execution units, in response to the launch instruction, use a key of the processor to authenticate the authenticated code module stored in the protected memory.

12. (Previously Presented) The processor of claim 1, wherein the execution units, in response to the launch instruction, decrypt at least a portion of the authentication module stored in the memory.

13. (Original) The processor of claim 1, wherein the execution units, in response to the launch instruction, decrypt at least a portion of the authentication module to obtain a digest value, and determine whether the authentication module is authentic based upon the digest value.

14. (Original) The processor of claim 1, wherein the execution units, in response to the launch instruction, obtain a digest value for the authentication code module, generate a computed digest value from at least a portion of the authenticated code module, and determine that the authenticated code module is authentic in response to the digest value and the computed digest value having a predetermined relationship.

15. (Original) The processor of claim 1, wherein the execution units, in response to the launch instruction, RSA-decrypt a signature of the authentication code module to obtain a digest value from the signature, perform a SHA-1 hash on the authenticated code module to generate a computed digest value, and determine that the authenticated code module is authentic in response to the digest value and the computed digest value being equal.

16. (Original) The processor of claim 1, wherein the execution units initiate execution of the authenticated code module only if the authenticated code module is determined to be authentic.

17. (Original) The processor of claim 16, wherein the execution units generate an error code in response to determining that the authenticated code module is not authentic.

18. (Original) The processor of claim 17, wherein the execution units generate a trap in response to determining that the authenticated code module is not authentic.

19. (Withdrawn) The processor of claim 1, wherein the execution units execute the authenticated code module from a execution point specified by one or more operands of the launch instruction.

20. (Withdrawn) The processor of claim 1, wherein the execution units execute the authenticated code module from an execution point specified by one or more fields of the authenticate code module.

21. (Withdrawn) The processor of claim 1, wherein the execution units mask one or more events selected from a group of events comprising INTR, NMI, SMI, INIT, and A20M events in response to executing the launch instruction.

22. (Previously Presented) The processor of claim 1, wherein the execution units authenticate and initiate execution of the authenticated code module stored in the memory in response to executing microcode associated with the launch AC instruction.

23. (Original) The processor of claim 1, embodied in a machine readable medium.

24. (Canceled)

25. (Withdrawn) The processor of claim 24, wherein the front end generates one or more ops for the instruction, and execution of the instruction results in the execution units executing the one or more ops.

26. (Withdrawn) The processor of claim 24 further comprising a processor key, wherein execution of the instruction results in the execution units authenticating the authenticated code module based upon the processor key.

27. (Canceled)

28. (Canceled)

29. (Canceled)

30. (Withdrawn) The processor of claim 28, wherein execution of the instruction results in the execution units initiating execution of the authenticated code module from an execution point specified by one or more operands of the instruction.

31. (Withdrawn) The processor of claim 24, wherein execution of the instruction results in the execution units initiating execution of the authenticated code module from an execution point specified by one or more fields of the authenticate code module.

32. (Canceled)

33. (Canceled)

34. (Canceled)

35. (Canceled)

36. (Canceled)

37. (Canceled)

38. (Canceled)

39. (Canceled)